مقدمة لتشفير البيانات والرسائل باستخدام

GnuPG

بسم اللّه الرحمن الرحيم

يحق لك نسخ ونقل هذا الكتيّب كيفما تريد

مهْدى لمجتمع لينكس العربي

http://www.linuxac.org

بركات

b4r4k47@hotmail.com
http://twitter.com/#!/B4r4k47

21 جماد الثاني 1432
Tuesday, May 24 2011

جدول المُحتويات

مدخل

في العالم الرقمي ينعدم الأمان. فاحتمال تعرض سريّة رسائلنا للانتهاك مرتفع. حيث يمكن لشركات البريد الإلكتروني الإطلاع على بريدنا. لا تكترث لإعلانات الخصوصيّة, فكم من أحداث حدثت أثبتت أن حماية الخصوصية التي يدعونها مجرد حبر على ورق. إضافة على هذا, نلاحظ انتشار إستخدام أدوات الهجوم على الشبكات كأدوات إلتقاط الحزم `sniffing` و أدوات التزوير `spoofing` ووصلت سهولتها إلى أن يتقن استخدامها طفل عمرة 10 أعوام.

هناك الكثير من الأدوات السهلة والقوية والمجانية أيضاً التي يمكنك استخدامها لزيادة خصوصيتك وحمايتك من تداعيات تلك الهجمات والتعديات على خصوصيتك ومن بين تلك الأدوات أداة `GNU Privacy Guard` أو اختصاراً `GnuPG`.

أداة GnuPG

أداة GnuPG أداة تشّفير وتوثيق مجانية ومفتوحة المصدر موافقة لمعيار التشفير OpenPGP المُستخدمة في تشفير البريد الإلكتروني والتواقيع الرقمية و منافسة لكثير من الأدوات التجارية والباهظة الثمن.متوافقة مع كثير من الأنظمة يمكنك عن طريقها تبادل الرسائل المُشفرة بين عائلتك أو أصدقائك أو عُملائك أو زملائك في العمل بكل سهولة. الأداة مُوجهة للأصل لنظام لينكس, لكن هناك عدة مشاريع مشتقة منها للأنظمة الأخرى مثل ويندوز و ماك وسنتعرّف أكثر عليها عن طريق هذا الكُتيّب إنشاء الله.

تحميل وتنصيب GnuPG

إذا كنت مستخدم ويندوز يمكنك تحميل ملف التنصيب عن طريق الصفحة :

http://gpg4win.org/download.html

وتنصيبه كالمعتاد, للبرنامج واجهة رسومية, لكننا سنستخدم الواجهة النصيّة فهمك لاستخدامها سيجعل فهم الواجهة الرسومية سهل جداً.

للتأكد من التنصيب اكتب المُضلل بخط عريض في سطر الأوامر :

```
> gpg --help
```

يفترض أن ترى قائمة المساعدة الخاصة بالبرنامج.

إذا كنت مُستخدم لينكس غالباً ما تكون منصبّة بشكل قياسي. إن لم تجدها, يمكنك أن تبحث في مُدير الحزم عن الحزمة gnupg وتنصبّها.

للتأكد من التنصيب اكتب المُضلل بخط عريض في الطرفيّة :

```
$ gpg --help
```

يفترض أن ترى قائمة المساعدة الخاصة بالبرنامج.

إذا كُنت مستخدم نظام التشغيل ماك, يمكنك تحميل ملف التنصيب عن طريق الصفحة :

http://www.gpgtools.org/installer/index.html

وتنصيبه كالمعتاد.

للتأكد من التنصيب اكتب المُضلل بخط عريض في الطرفيّة :

```
$ gpg --help
```

يفترض أن ترى قائمة المساعدة الخاصة بالبرنامج.

المفتاح العام والمفتاح الخاصّ

قبل البدء يجب أن نفهم طريقة إستخدام التشفير بالمفاتيح المتناظرة بشكل عام. أول ما تبدأ به عند إستخدام هذا النوع من التشفير هو توليد مفتاحين, الأول يسمّى المفتاح الخاص `Private Key`. والآخر يسمّى المفتاح العامّ `Public Key`. المفتاح الخاص تبقيّة محفوظ لديك ولا تعطيه لأحد.

أما المفتاح العامّ, يمكنك أن تعطيه وترسله لمن تشاء. ويمكنك حتّى أن تضعه على موقعك دون أي قلق. من يريد إرسال رسالة أو ملف لك يرسلها مشفرة بالمفتاح العامّ. إذا وصلت لك, تفكّ تشفيرها بالمفتاح الخاصّ. وإذا أردت أن ترسل لأحد, استخدم مفتاحه العام. هذه الطريقة ببساطة :).

الرسالة المُشفرة بالمفتاح العامّ لن يستطيع أي مفتاح فك تشفيرها سوى المفتاح الخاصّ الذي ينتمي له المفتاح. والعكس صحيح,الرسالة المُشفرة بالمفتاح الخاصّ لن يستطيع أي مفتاح أي يفك تشفيرها سوى بالمفتاح العامّ الذي ينتمي له.

توليد المفتاح الخاص

كما ذكرنا, أننا أولاً بحاجه لتوليد المفاتيح, العام والخاص. يمكننا عمل هذا عن طريق الخيار `gen-key--` وسيسألنا GPG بعض الأسئلة قبل التوليد :

```
$ gpg --gen-key
gpg (GnuPG) 1.4.11; Copyright (C) 2010 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
  (1) RSA and RSA (default)
  (2) DSA and Elgamal
  (3) DSA (sign only)
  (4) RSA (sign only)
Your selection? 1
```

يسألك عن نوع المفتاح الذي نريد توليده, سنختار الخيار الأوّل "`RSA and RSA`" والمشار إليه بكلمة `default`. اكتب 1 أو اضغط على زرّ الإدخال مباشرة.

```
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048)
```

سيسألك عن طولّ المفتاح, كلما زاد طول المفتاح كلما كان أفضل. لكن لن نجعل المفتاح يبقى للأبد, بل سنجعله صالح لعام فقط لذا 2048 مناسب. فقط اضغط على زرّ الإدخال.

```
Requested keysize is 2048 bits
Please specify how long the key should be valid.
      0 = key does not expire
    <n>  = key expires in n days
    <n>w = key expires in n weeks
    <n>m = key expires in n months
    <n>y = key expires in n years
Key is valid for? (0) 1y
```

سيسألنا عن عُمر المفتاح (حيث n يعني رقمّ) :

إذا كتبت 0 يعنيّ أن المفتاح لن ينتهي بل سيدوم صالح للأبد.

إذا كتبت n يعنيّ أن المفتاح سيدوم لأيام days تساوي هذا الرقم.
مثلاً إذا كتبت 10 يعني أنه سيدوم 10 أيام وينتهي بعدها (ستحتاج لتوليد آخر جديد).

إذا كتبت nw يعنيّ أن المفتاح سيدوم لأسابيع weeks تساوي هذا الرقم.
مثلاً إذا كتبت w 10 يعني أنه سيدوم 10 أسابيع وينتهي بعدها (ستحتاج لتوليد آخر جديد).

إذا كتبت nm يعنيّ أن المفتاح سيدوم لأشهر months تساوي هذا الرقم.
إذا كتبت ny يعنيّ أن المفتاح سيدوم لسنين years تساوي هذا الرقم.

كلما زادت درجة سرية المعلومات المُتبادلة, قلل الأيام. سأختار سنه أجدها مناسبه.

```
Key expires at Thu 23 May 2012 07:17:55 AM AST
Is this correct? (y/N) y
```

سيعطيك تاريخ انتهاء المفتاح ويسألك ما إن كنت متأكد من أن هذا ما تريده. اكتب y للتأكيد و N للنفي.

```
You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
  "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"
```

```
Real name: B4r4k47
```

سيسألك عن اسمك, اكتبه ثمّ اضغط على زر الإدخال.

```
Email address: b4r4k47@hotmail.com
```

اكتب بريدك الإلكتروني.

```
Comment:
```

إذا أردت أن تكتب تعليق أو أي شيئ اكتبه وإلا اتركه فارغ.

```
You selected this USER-ID:
  "B4r4k47 <b4r4k47@hotmail.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
```

سيسألك أن تؤكّد صحة المعلومات التي كتبتها, إذا كان هناك خطأ:

في الاسم, اكتب N وصححه.
في التعليق, اكتب C وصححه
في البريد, اكتب E وصححه.

إذا كان كل شيئ صحيح اكتب O. واضغط على زر الإدخال.

```
You need a Passphrase to protect your secret key.
Enter passphrase:
Repeat passphrase:
```

سيطلب منك أن تدخل كلمة سرّ لحماية مفتاحك الخاص. أكتبها وأعد كتابتها مرة أخرى للتأكيد (لاحظ أنها لن تظهر بل مخفيه).

```
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
+++++
+++++.....++++++
....+++++
...+++++
gpg: key 985C517A marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: public key of ultimately trusted key 284D2D7B not found
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   2  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 2u
gpg: next trustdb check due at 2012-05-23
pub  2048R/985C517A 2011-05-24 [expires: 2012-05-23]
   Key fingerprint = 0F6B 3FCB C827 2B25 407B  4988 0AAE 1B07 985C 517A
uid                  B4r4k47 <b4r4k47@hotmail.com>
sub   2048R/3E428AF5 2011-05-24 [expires: 2012-05-23]

$
```

الآن ستبدأ عملية توليد المفتاح انتظر حتى تنتهي وحرك الفأرة أو كبر وصغر النوافذ أثناء هذه العملية, إذا انتهت ستعود للطرفيّة. قد تتوقف عملية التوليد وتظهر رسالة مشابهة لهذه الرسالة :

```
Not enough random bytes available.  Please do some other work to give
the OS a chance to collect more entropy! (Need 86 more bytes)
```

فقط قم يتحرك الفأرة أو قم بتكبير وتصغير الشاشة, المهمّ أن تقوم بأي نشاط كي تكتمل. لأن المفتاح يتولّد عن طريق حسابات عشوائية مثل موضع الشاشة حركة الفأرة .. ألخ.

إظهار المفتاح العام الخاص بنا

كما ذكرنا, أننا نحتاج لمفتاحين خاص وعام. الخـاص قمنـا بتوليـده وحفـظ فـي الجهـاز بقـي أن نظهـر المفتـاح العـام كـي نسـتطيع مشـاركته مـع الآخـرين. لنستعرض المفاتيح التي لدينا أولاً بالخيار `list-key--` هكذا:

```
$ gpg --list-key
/home/B4r4k47/.gnupg/pubring.gpg
--------------------------------
pub   2048R/92892F27 2011-05-24 [expires: 2012-05-23]
uid                  B4r4k47 <b4r4k47@hotmail.com>
sub   2048R/20BDF728 2011-05-24 [expires: 2012-05-23]
$
```

جميل. لنصدّر مفتاحنا العام بهذا الأمر :

```
$ gpg --armor --export
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.11 (GNU/Linux)

mQENBE3bQXUBCAC9Fv/hdc4GjoWU8NQv+HE18NphR8y06OfrOMARde7z+KwROJOQ
iejIU+hyy2znglI9SEDnPXay2GMPIZp+tJ0QKVxpUIYw0HF3A+2zroxz9Dc8uyux
PJe+7z/HCsv2F7q3JmGy42xLaB2bLem8cRPjgQ9k3MUSkajoevUCht4npwljOg04
5 OK0HHV/UhpMBl5+IWWlVcTCtjXmA/cN38pmWhRanXJHRbMbd+IN9Qw4h+uim52h
gJSHrfBvv4dVTsOtxiNwt4/Vcn1elnvo+Dyzeu1qxC74g790xnsHksIYORiAV7do
LTfjmpwyoO+XweiOmWRD4A0o8FskVadYR99fABEBAAG0HUI0cjRrNDcgPGI0cjRr
NDdAaG90bWFpbC5jb20+iQE+BBMBAgAoBQJN20F1AhsDBQkB4TOABgsJCAcDAgYV
CAIJCgsEFgIDAQIeAQIXgAAKCRDe+gWrkokvJ3MFB/0X6IuhUHW1F8eahHudA0K7
bDSj+0NhRmlX0L8nsDn5DT7UY0b0aCvDT925eMprKiKjXDg+vnsPCenyAx82HQGW
YISNVvJca8QbKDGxJoEhqK1pySjzCWrTobqpg4aMX2A6johd6amFyLpU3fpAp78e
oYjEYgyLxU7ULPIFMts0tQ8kfQTwIv6oB8N3JXlczisdsW7/OM8l8FMJ5Glq2zY3
BfiyN+e9szHUXyIWj63fj0UFMb8dKpvZ2p/6KPuZjh7JvjifDMcOsxmTuMsnCuiP
EYlMfOM3Bk1Ibyw8bzv9FfpYS9SBm+SwVhxTJqCvy0w4saftWiErrQZMU2fmG2OZ
uQENBE3bQXUBCAC7Y1EslkJ3AWmJBjJYlomD8qphNAORyvZ2lMFDMyya90ZtyfX3
lP2mw72ol1xzg2Ot+CjpR5gt5g4p0Hxh3N2q6bTLoQ+EnxdwNJmho2R2GCgEVkbI
UuCHXg10Tqb5+LSqxpFKbxHlSjlSDJUCg9pvQ/5hgijii1bmsmTBoLTe5puQ39NL
pIg2NxWzynlnM7CWm6WzcVjWVcQsHiz0JmJLwWSozfbhxDE4FvXPrRpt6w63FYAY
IIdMnW7p2n9/nEmVz3MtMXgYol6j7YS5OMZM7qrJroFLN6qmZIboPuagzeRwH2EN
g/ubxSU0lmz5WRfzfwlphd4TryVlWIUYF7VrABEBAAGJASUEGAECAA8FAk3bQXUC
GwwFCQHhM4AACgkQ3voFq5KJLycckAgAnUeO3B+qbQiimL0ExTPLGKvGSeImkfC7
2 ZfrIWRRBdg57p09rl1O8JgXVA8GaGSvLDQ3SAz/PSz7LRHlxX6CEheYCoccFuzS
5 JTe5thZJpGEhyygYEF4uq8Luen+r7PTvYuZMrVQhZvAKW4RBgrLJaCNPXIOUDau
qd57G2tfcLXj4UlKTCs01K41UDRA7bHA2W9ptxP9WHYzNG4F4vNQ58RDgSJCwegm
6 j1baH94gcg5Nldlzd8gDFjBN5dlj055o54RNW+whZYT2Ivtk2cWWUP57o7ZNxPU
KajEiLqGKmuW2hTEcD1SKIrXRQ4iUzgcEyNuuimqu0f0bqRIYSQcRg==
=EeKM
-----END PGP PUBLIC KEY BLOCK-----
$
```

هكذا يبدو مفتاحنا العام :). انسخه وضعه في ملف أو يمكنك ببساطه كتابة :

```
$ gpg --armor --export > publickey.txt
```

وستجد المفتاح في الملف `publickey.txt`. ضعه في مكان عام مثل موقعك أو تسلمه لصديقك عن طريق وسيط آمن لأنه مـن الممكـن أن يعـترض أحـد المفتاح ويقوم بتبديله بالمفتاح الخاص به.

استعراض المفاتيح المُخزنة

كما ذكرنا في المثال السّابق, الخيار list-key-- مُهمته استعراض كافة المفاتيح العامة المُخزنة في جهازك :

```
$ gpg --list-key
/home/B4r4k47/.gnupg/pubring.gpg
--------------------------------
pub   2048R/92892F27 2011-05-24 [expires: 2012-05-23]
uid                  B4r4k47 <b4r4k47@hotmail.com>
sub   2048R/20BDF728 2011-05-24 [expires: 2012-05-23]
$
```

سيظهر لنا اسم صاحب المفتاح وبريده الإلكتروني وتاريخ انتهاء المفتاح. ويمكن إن تضيف عليه اسم صاحب المفتاح كي تعرف تفاصيل حول مفتاح مُعيّن إذا كان لديك عدّة مفاتيح مُخزّنة :

```
$ gpg --list-key B4r4k47
pub   2048R/92892F27 2011-05-24 [expires: 2012-05-23]
uid                  B4r4k47 <b4r4k47@hotmail.com>
sub   2048R/20BDF728 2011-05-24 [expires: 2012-05-23]
```

أو عن طريق بريده الإلكتروني :

```
$ gpg --list-key b4r4k47@hotmail.com
pub   2048R/92892F27 2011-05-24 [expires: 2012-05-23]
uid                  B4r4k47 <b4r4k47@hotmail.com>
sub   2048R/20BDF728 2011-05-24 [expires: 2012-05-23]
```

إضافة المفاتيح

إذا أردت إضافة مفتاح عام لقائمة المفاتيح, يمكنك عمل هذا بتمرير الخيار import-- متبوع بمسار هذا المفتاح, على سبيل المثال, أعطاك صديقك رابط موقعه الذي يحوي مفتاحه العام http://www.friend.org/friend.txt, لنرى هذا المفتاح :

```
$ curl http://www.friend.org/friend.txt
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.10 (GNU/Linux)

mI0ETdtXjgEEANUtsrzQun8ZemKxbgn+o35pkXuVcH8hwLhackaHXnXCnkj7TfA/
Y9TwZZXQyvwZiBG2JxbWtjBe4qif31QaX50zKjnEkRhbuuCjG4uRtcmFyT5IWw3G
eZmln+wDyqj75Bof91GWijMtINlb4vnhBhtfATDykwZtnODJgnHoxfcpABEBAAG0
F0ZyaWVuZCA8bWFpbEBnbWFpbC5jb20+iLgEEwECACIFAk3bV44CGwMGCwkIBwMC
BhUIAgkKCwQWAgMBAh4BAheAAAoJEBBEfRNXADYT8WcD/jqIs/FZPnJx7C0UgvdN
HJPo7tyGN2751kOO15pTiTggVQCDm3tUC6MP8JtAPTf1UVHZE+F+WTyzG3UusAMm
r+bJ6Iwn90yixzI3kPBEj3WL/OY/PfzIFUhGbXE5293abMb/0Kv6NRMYEIwrX6KX
7 OxwLhACIQVFSbr8t308WfT5uI0ETdtXjgEEALvPKgxLQmnuJsJVnj9MafZ0Du8j
Hsikq3QmUznPRNeicbz1zbkAYLP4rj7YteuuxekyazD3XSJpD7i4/O/wdPdJyGaA
w4dS5cRiQ0nEntpMrO5SkLcjvF7roGC4cjt7V0HyUbqYrb+R5pYNigSmOOmmfs4w
2 pqgOL1EZuytywjlABEBAAGInwQYAQIACQUCTdtXjgIbDAAKCRAQRH0TVwA2E+h8
A/9Hlu+PE3fFb43QfsMRQnzCsml1X0lobYnjEOwF0Mx2rLkU3f8sQbGBGWYuDRSC
oYOq68hSx9qy44QfPYvQpy6pcpAPPzNGZqsGrT+85Xz/T5bdJnj39F05f4lx1wBP
iAvHawOCtXuzdrssS7fql1FrpEgFBk3FtIttJ5co+AiKeg==
=Xrug
-----END PGP PUBLIC KEY BLOCK-----
$
```

لإضافة هذا المفتاح لديك, قم بتحميله عن طريق wget مثلاً :

```
$ wget http://www.friend.org/friend.txt
--2011-05-24 10:07:26-- http://www.friend.org/friend.txt
Resolving www.friend.org... 192.168.150.142
Connecting to www.friend.org|192.168.150.142|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1008 [text/plain]
Saving to: “friend.txt”

100%[======================================>] 1,008      --.-K/s   in 0s

2011-05-24 10:07:26 (58.3 MB/s) - “friend.txt” saved [1008/1008]
$
```

بعد أن قمنا بتحميله, نضيفه لقائمة المفاتيح بالشكل التالي :

```
$ gpg --import friend.txt
gpg: key 57003613: public key "Friend <mail@gmail.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
$
```

كما رأينا, ظهرت لنا تفاصيل عن المفتاح كإسم صاحب المفتاح العام وبريده الإلكتروني. لنستعرض المفاتيح التي لدينا بعد أن أضفناه:

```
$ gpg --list-key
/home/B4r4k47/.gnupg/pubring.gpg
--------------------------------
pub   2048R/92892F27 2011-05-24 [expires: 2012-05-23]
uid                  B4r4k47 <b4r4k47@hotmail.com>
sub   2048R/20BDF728 2011-05-24 [expires: 2012-05-23]

pub   1024R/57003613 2011-05-24
uid                  Friend <mail@gmail.com>
sub   1024R/7C9A5B0A 2011-05-24

$
```

كما نرى, مفتاح Friend أصبح في القائمة.

في حالات قد تضيف مفتاح مثل هذا المفتاح :


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3ia

mQCNAjPC3egAAAEEAO1vs4jyGRorCdJkqQyE7R/ImbBdh9N/UTsoNBKRS2WMM9h0
oN4ItQ5phzdXwtv3qsd0oy2LQNA4YtFoheEKv66Yqbt2/9NZDhotHL8HB1tAa07v
pATS+wnJlokN8ul3bkYANCXIFjkFiXH+18eE5VImV+TaEVdX2vY84gaS8LkFAAUR
tCNUaGVvIGRlIFJhYWR0IDxkZXJhYWR0QG9wZW5ic2Qub3JnPokAlQMFEDQwHOK9
KQY4dodZBQEBSvwD/2SHnQW3c00Q19a96jvEipa4J7cXQCoJkm9WME5Oaxc7H7of
FT2HrKQCL3iQJEQlWxwJnccAFcZvybIi3VNTdUgPuRM9i3dGLvHosS4mVk/5q3/t
2 OCTMwQTfOMvFyylHQ54uDhyQ3l5XyNSCiAG7773rLIy8PQIgVBkbgpup5nHiQEV
AwUQNDAcz3crsxJuc7vBAQHD7gf/Z5sR1aQ1ETgxCtbiugKuIE+rMekaJayRADSI
fFFaK7psf77o6wUIF9aNTfoaCHH/mc1kOzzmi/iqlO3058lZjGUISYrCYVfljjAg
NUvMBBhFMS5fia1vgyxvUE3uAqpCyYNbLai6xQ3bJwk5tEOVyQEW6Zl+AHia4TqY
XE5TeB+ShVVP/GJfqxn2W3LoAqEC6buZuCZLnUrDnynZlMpZNqfT3YRYGCeWT6GT
G7p/B183Q7K4ydB5KbEsOIwZbT26CdyQz9ldOMyUv6F/794nYywVXDMAie/Qvv3s
ppgm9vt228kfhalxpJYjotQk8YH8unt8f8WH8AhCT9e7IkGJi4kAlQMFEDQwG+/2
POIGkvC5BQEBDnsEAKeDaL76HZTmcXwpx23zUv/fUxDWhMHgsG1bux4Yr7HN0wes
KGLCzAQCowpvXs8wVSmA1JdU0FA3aAdRmBICugn47FGn2BoOgmXEhIiwlWd98Oee
sXrAbqkDdo6bFXKObaMfL89FbgQwLHWvSPDpZM4R5G8Rl2f77i4QlF6opTmv
=tHdO
-----END PGP PUBLIC KEY BLOCK-----
```

ويظهر لك تحذير عند إضافته كهذا :

```
$ gpg --import pgpkey.txt
gpg: WARNING: digest algorithm MD5 is deprecated
gpg: please see http://www.gnupg.org/faq/weak-digest-algos.html for more information
gpg: key 92F0B905: public key "Theo de Raadt <deraadt@openbsd.org>" imported
gpg: Total number processed: 1
gpg:               imported: 1  (RSA: 1)
gpg: public key of ultimately trusted key 284D2D7B not found
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   2  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 2u
gpg: next trustdb check due at 2012-05-23
$
```

المفتاح سليم ولو استعرضت قائمة المفاتيح ستجده قد أضيف لكنّ التحذير سببه أن المفتـاح ضـعيف كحالـة اسـتخدامه لخوارزميـة تشـفير ضـعيفه أو طـوله صغير فقط.

استعراض وتصدير المفاتيح العامة الخاصة بالآخرين

قد تريد مثلاً نقل مفتاح أو تخزينه في قرص دون أن تعيد طلبه من صاحب هذا المفتاح, يمكنك أن تعملها بنفس الطريقة التي تستخرج بها مفتاحك العام فقط اكتب اسم أو بريد صاحب هذا المفتاح وسيطبعه :

```
$ gpg --armor --export deraadt@openbsd.org
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.11 (GNU/Linux)

mQCNAjPC3egAAAEEAO1vs4jyGRorCdJkqQyE7R/ImbBdh9N/UTsoNBKRS2WMM9h0
oN4ItQ5phzdXwtv3qsd0oy2LQNA4YtFoheEKv66Yqbt2/9NZDhotHL8HB1tAa07v
pATS+wnJlokN8ul3bkYANCXIFjkFiXH+18eE5VImV+TaEVdX2vY84gaS8LkFAAUR
tCNUaGVvIGRlIFJhYWR0IDxkZXJhYWR0QG9wZW5ic2Qub3JnPokAlQMFEDQwHOK9
KQY4dodZBQEBSvwD/2SHnQW3c00Q19a96jvEipa4J7cXQCoJkm9WME5Oaxc7H7of
FT2HrKQCL3iQJEQlWxwJnccAFcZvybIi3VNTdUgPuRM9i3dGLvHosS4mVk/5q3/t
2OCTMwQTfOMvFyylHQ54uDhyQ3l5XyNSCiAG7773rLIy8PQIgVBkbgpup5nHiQEV
AwUQNDAcz3crsxJuc7vBAQHD7gf/Z5sR1aQ1ETgxCtbiugKuIE+rMekaJayRADSI
fFFaK7psf77o6wUIF9aNTfoaCHH/mc1kOzzmi/iqlO3058lZjGUISYrCYVfljjAg
NUvMBBhFMS5fia1vgyxvUE3uAqpCyYNbLai6xQ3bJwk5tEOVyQEW6Zl+AHia4TqY
XE5TeB+ShVVP/GJfqxn2W3LoAqEC6buZuCZLnUrDnynZlMpZNqfT3YRYGCeWT6GT
G7p/B183Q7K4ydB5KbEsOIwZbT26CdyQz9ldOMyUv6F/794nYywVXDMAie/Qvv3s
ppgm9vt228kfhalxpJYjotQk8YH8unt8f8WH8AhCT9e7IkGJi4kAlQMFEDQwG+/2
POIGkvC5BQEBDnsEAKeDaL76HZTmcXwpx23zUv/fUxDWhMHgsG1bux4Yr7HN0wes
KGLCzAQCowpvXs8wVSmA1JdU0FA3aAdRmBICugn47FGn2BoOgmXEhIiwlWd98Oee
sXrAbqkDdo6bFXKObaMfL89FbgQwLHWvSPDpZM4R5G8Rl2f77i4QlF6opTmv
=tHdO
-----END PGP PUBLIC KEY BLOCK-----
$
```

حذف المفاتيح

إذا أردت حذف مفتاح عام, كحالة انتهائه أو لم تعد بحاجه إليه, استخدم الخيار delete-keys-- متبوع باسم صاحب المفتاح أو بريده, كما في المثال :

```
$ gpg --delete-keys Friend
gpg (GnuPG) 1.4.11; Copyright (C) 2010 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.


pub  1024R/57003613 2011-05-24 Friend <mail@gmail.com>

Delete this key from the keyring? (y/N) y
$
```

سيطلب منك فقط أن تؤكّد أنك تريد فعلاً حذف المفتاح اضغط على الزرّ y. ولو استعرضت الآن لائحة المفاتيح لن تجده بها.

إذا أردت حذف مفتاحك لسبب ما, احذف المفتاح الخاص أولاً هكذا :

```
$ gpg --delete-secret-keys B4r4k47
gpg (GnuPG) 1.4.11; Copyright (C) 2010 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.


sec  2048R/985C517A 2011-05-24 B4r4k47 <b4r4k47@hotmail.com>

Delete this key from the keyring? (y/N) y
This is a secret key! - really delete? (y/N) y
$
```

ثمّ احذف المفتاح العام, فلم تعد هناك حاجه له :

```
$ gpg --delete-keys B4r4k47
gpg (GnuPG) 1.4.11; Copyright (C) 2010 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.


pub  2048R/985C517A 2011-05-24 B4r4k47 <b4r4k47@hotmail.com>

Delete this key from the keyring? (y/N) y
$
```

تشفير الملفات

بعدّ أن تعلمنا الأساسيات التي نحتاجها بشكل دائم, حان الوقت لتعلّم كيفية تشفير الملفات وفكّ تشفيرها. لتشّفير ملف نصّي أو صورة أوي أي ملف نستخدم الأمر encrypt-- متبوع بمسار هذا الملف كما في المثال :

```
$ gpg --encrypt privet.pdf
You did not specify a user ID. (you may use "-r")

Current recipients:

Enter the user ID.  End with an empty line: B4r4k47

Current recipients:
2048 R/20BDF728 2011-05-24 "B4r4k47 <b4r4k47@hotmail.com>"

Enter the user ID.  End with an empty line:
$
```

سيطلب منك إدخال المفتاح الذي تريدّ استخدامه, كتبنا مثلاً B4r4k47 سيظهر لنا تفاصيل هذا الحساب كتأكيد ففي حالات قد تختلط عليك الأمور خصوصاً عند تشابه الأسماء. إذا تأكدت من أن هذا الاسم الذي تريد إستخدام مفتاحه اضغط على زرّ الإدخال أو استخدم البريد الإلكتروني فمن المعروف أن البريد الإلكتروني لا يتشابه وسيتّم تشفير الملف وسينتج ملف بنفس اسم الملف الأصلي يحمل الامتداد gpg وهو الملف المشفر الذي ترسله:

```
$ ls privet.*
privet.pdf  privet.pdf.gpg
```

قد تودّ تغيير اسم الملف الناتج كي لا يعرف أحد أي تفصيل عن نوع أو طبيعة هذا الملف ولا يستطيع تحديد درجة أهميته, فبدل أن تعيد تسميته يمكنك كتابة out-- متبوع باسم الناتج :

```
$ gpg --out file --encrypt privet.pdf
You did not specify a user ID. (you may use "-r")

Current recipients:

Enter the user ID.  End with an empty line: b4r4k47@hotmail.com

Current recipients:
2048 R/20BDF728 2011-05-24 "B4r4k47 <b4r4k47@hotmail.com>"

Enter the user ID.  End with an empty line:
$
```

الآن لو استعرضت الملفات, ستجد ملف جديد نتج باسم file وهو الملف المشفر :

```
$ ls | grep file
file
$
```

إذا أردت عملية التشفير صامته غير تفاعلية يمكنك تمرير الخيار r- متبوع باسم أو بالبريد الإلكتروني الخاص بصاحب المفتاح كالتالي:

```
$ gpg -r B4r4k47 --out important --encrypt message.txt

$
```

كما ترى, شُفر الملف مباشرة. يفيد هذا كثيراً عند إستخدام gpg عند كتابتك لمخطوطة script مثلاً.

فك تشفير الملفات

لفك تشفير ملف مُشفر نستخدم الخيار decrypt--. أولاً لننشئ ملف بسيط اسمه file.txt مكتوب داخله كلمة Demo :

```
$ echo "Demo" > file.txt
$ cat file.txt
Demo
$
```

لنشفره في ملف اسمه important كما تعلمنا وسنحذف الملف الأصلي :

```
$ gpg -r B4r4k47 --out important --encrypt file.txt
$ rm file.txt
```

الآن على افتراض أن وصلنا الملف المشفر important عن طريق البريد, لقراءته نفكّ تشفيره عنه أولاً هكذا :

```
$ gpg --decrypt important
You need a passphrase to unlock the secret key for
user: "B4r4k47 <b4r4k47@hotmail.com>"
2048-bit RSA key, ID 20BDF728, created 2011-05-24 (main key ID 92892F27)


Enter passphrase:
```

أدخل كلمة السر الخاصة بمفتاحك الخاص.

```
gpg: encrypted with 2048-bit RSA key, ID 20BDF728, created 2011-05-24
   "B4r4k47 <b4r4k47@hotmail.com>"
Demo
$
```

كما لاحظت, طُبعت محتويات الملف important بعد فكّ تشفيره على الشّاشة ! لكن قد تودّ حفظ الناتج في ملف. لذا مرر الخيار out-- كالتالي :

```
$ gpg --out file.txt --decrypt important

You need a passphrase to unlock the secret key for
user: "B4r4k47 <b4r4k47@hotmail.com>"
2048-bit RSA key, ID 20BDF728, created 2011-05-24 (main key ID 92892F27)

gpg: encrypted with 2048-bit RSA key, ID 20BDF728, created 2011-05-24
   "B4r4k47 <b4r4k47@hotmail.com>"
$ cat file.txt
Demo
$
```

فكما ذكرنا, لأنّ الملف important مُشفر بالمفتاح العام, بالتأكّيد سيُفك تشفيره بالمفتاح الخاص والمفتاح الخاص دائماً يتطلب استخدامه كلمة مرور حتّى إذا سُرق فمن سرقه يحتاج لكلمة السر كي يستطيع استخدمه.

سيناريو إرسال رسالة مُشفّرة

أردت أن أرسل لصديقي زياد رسالة عبارة عن ملف نصّي اسمه server_password.txt تحوي حساب و كلمة مُرور لخادم كي يستطيع الاتصال بخادمي عن طريق الـ SSH ومحتويات الرسالة كالتالي :

```
[B4r4k47@IronSystem]$ cat server_password.txt
IP        : 192.168.150.142
USER      : Zeiad
PASSWORD  : dd#@(3jh! %
[B4r4k47@IronSystem]$
```

كما نرى بيانات كهذه من الخطر جداً أن نرسلها بهذا الشكل, ولو حتى بالبريد فمن المُمكن جداً أن يعترضها أحد ما عن طريق إلتقاط الحزم sniffing أو التزوير spoofing ونحن لا نظمن أن زياد سيستخدم الاتصال الآمن SSL بشكل صحيح لذا من المُهمّ جداً أن نُشفرها حتى نظمن أنها لـن تفتـح إلا عـن طريق زياد وإن وصلت لغيره فلن يستفيد منها لأنه لن يستطيع فكّ التشفير. أول ما سأقوم به هو أخذ مفتاح زياد العام والموجود على مُوقعه الشخصي.

```
[B4r4k47@IronSystem]$ wget http://zeiad-blog.org/mykey.txt
--2011-05-24 13:18:52-- http://zeiad-blog.org/mykey.txt
Resolving zeiad-blog.org... 192.168.150.142
Connecting to zeiad-blog.org|192.168.150.142|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1727 (1.7K) [text/plain]
Saving to: “mykey.txt”

100%[======================================>] 1,727     --.-K/s   in 0s

2011-05-24 13:18:52 (36.5 MB/s) - “mykey.txt” saved [1727/1727]
[B4r4k47@IronSystem]$
```

بعدما حملته, أضفته لقائمة المفاتيح :

```
[B4r4k47@IronSystem]$ gpg --import mykey.txt
gpg: key B05B625E: public key "Zeiad <zeiad@zeiad-blog.org>" imported
gpg: Total number processed: 1
gpg:              imported: 1  (RSA: 1)
```

الآن يمكن أن أنشفر هذا الملف بهذا المفتاح :

```
[B4r4k47@IronSystem]$ gpg -r Zeiad --out important --encrypt server_password.txt
[B4r4k47@IronSystem]$
[B4r4k47@IronSystem]$ ls -l important
-rw-r--r-- 1 B4r4k47 B4r4k47 404 May 24 13:20 important
[B4r4k47@IronSystem]$
```

الآن يمكنني أن أرسل الملف important كمرفق مع رسالة بريد بأمان ولن يستطيع أحد فكّ تشفيرها عدا زياد.

سيناريو فك تشفير الرسالة المُشفّرة

فتح زياد بريده الإلكتروني ووجد الرسالة :

From	b4r4k47@hotmail.com
To	zeiad@zeiad-blog.org
Subject	اللي طلبته

السلام عليكم ورحمة الله وبركاته

شيّك على المرفقات.. شيء يخصك ;)

3> سلام

ملف مرفق : <important>

سيقوم بتحميل الملف important ثمّ سيفك تشفيره بمفتاحه الخاصّ :

```
zeiad@DarkStart:~$ gpg --decrypt important

You need a passphrase to unlock the secret key for
user: "Zeiad <zeiad@zeiad-blog.org>"
2048-bit RSA key, ID 7124CBCB, created 2011-05-24 (main key ID B05B625E)

gpg: gpg-agent is not available in this session
gpg: encrypted with 2048-bit RSA key, ID 7124CBCB, created 2011-05-24
    "Zeiad <zeiad@zeiad-blog.org>"
IP        : 192.168.150.142

USER      : Zeiad

PASSWORD  : dd#@(3jh!%

zeiad@DarkStart:~$
```

كما رأيت, تبادلنا الملف المّهمّ بكل أمان فالملف كان مُشفر طوال تواجده على الشبكة العنكبوتية. ولم يكن بدون تشفير سوى على جهازي لحظة تشفيره وعلى جهاز زياد لحظة فك تشفيره.

الخاتمة

احرص كثيراً على إستخدام طرق وتقنيات تبادل المعلومات ألآمنـة مثـل الـ GPG و SSL و SSH و SFTP وعلّم أهلـك وأصـدقائك علـى اسـتخدامها. إن لـم تحميك فلن تضرك وربما ستجنّبك بعد إذن الله كثيراً من المشاكل التي أنت فى غناً عنها.

إذا وجدت إستخدام GNU Privacy Guard معقد قليلاً خصوصاً لأنه بدون واجهة رُسومية, فمـع الاسـتخدام المتكـرر سـيكون عـادي جـداً. أتقنتـه خلال كتابتي لهذا الكتيبّ :).

أتمنى أنك وجدت ولو فائدة قليلة من قراءة هذا الكُتيّب البسيّط. سائلاً الله لي ولك التوفيق والنجاح في الدنيا والآخرة.

المراجع

ويكيبيديا بي جي بي :

http://ar.wikipedia.org/wiki/%D8%A8%D9%8A_%D8%AC%D9%8A_%D8%A8%D9%8A

Wikipedia GNU Privacy Guard:

http://en.wikipedia.org/wiki/GNU_Privacy_Guard

Gnu Privacy Guard (GnuPG) Mini Howto (English):

http://www.dewinter.com/gnupg_howto/english/GPGMiniHowto.html


```
$ man gpg
```

الأمر cat يقابل في ويندوز type

الأمر ls يقابل في ويندوز dir